The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
2/9/2010

SUBJECT:
Vulnerabilities in the Microsoft SMB Client Could Allow Remote Code Execution (MS10-006)

OVERVIEW:
Two vulnerabilities have been discovered in the Microsoft Server Message Block (SMB) client that could allow a remote attacker to take complete control of a vulnerable system. SMB is used to provide shared access to files, printers, serial ports, and other miscellaneous communication between network devices. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining SYSTEM-level privileges. An attacker could then install programs; view, change, or delete data; or create new accounts.

SYSTEMS AFFECTED:

Windows 2000
Windows XP
Windows Vista
Windows 7
Windows Server 2003
Windows Server 2008

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Two vulnerabilities have been identified in the Microsoft Server Message Block (SMB) client that could allow remote code execution. SMB is used to provide shared access to files, printers, serial ports, and other miscellaneous communication between network devices.

The first issue is a kernal pool memory corruption vulnerability in the SMBv1 implementation on Windows 2003 and below. The vulnerability occurs when the client processes certain packet fields. The second issue is a race condition vulnerability in the SMBv1 implementation on Windows Vista and above. The vulnerability occurs when the client processes the SMB 'response' packet during the SMB client/server negotiation process. Authentication is not required to exploit either of these vulnerabilities.

Successful exploitation of these vulnerabilities could result in an attacker gaining SYSTEM-level privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the appropriate patch provided by Microsoft immediately after appropriate testing.
- Implement egress and ingress filtering for TCP ports 139 and 445 at your network perimeter.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:
Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-006.mspx
http://blogs.technet.com/srd/
http://blogs.technet.com/msrc/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0016
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0017

Secunia:
http://secunia.com/advisories/38500/

SecurityFocus:
http://www.securityfocus.com/bid/38093
http://www.securityfocus.com/bid/38100